SPECIFICATION AMENDMENTS

In the Detailed Specification, on page 13, the paragraph starting at line 20, replace the paragraph with the following:

> Shown attached to document verifier / validation terminal 12 are a fingerprint reader 14, iris scanner 15, and a camera 16. Depending upon the specific application of a terminal 12 some or all of these attachments may not be provided. In addition, although not shown in Fig. 1, document creation terminal 13 may have ones of a fingerprint reader 14, iris scanner 15, and a camera 16 attached thereto to gather biometric information from an applicant for a new document to be used in verifying the identity of the applicant.

In the Detailed Specification, on page 15, the paragraph starting at line 23, replace the paragraph with the following:

> A fingerprint reader 14 is used to capture a fingerprint of a document applicant for document presenter to be used to verify their identity, or to be compared to a fingerprint stored on the document. If further verification of the document applicant or presenter is required the fingerprint may be forwarded via verification system communication bus 11 and verification system server 10 to a trust authority to be processed in the same way as described in the previous paragraph. The fingerprint database to be utilized most likely is the FBI database and the fingerprint captured by a reader 14 is forwarded by bus 11, and server 10 to trust authority server [[~~22~~]] 28f. Server [[~~22~~]] 28f determines that the FBI database is to be accessed for the verification and forwards a request over secure government network 29 through gateway 38g to the FBI server 35 where the fingerprint for the identified document applicant or presenter is retrieved and returned to trust authority server[[~~22~~]] 28f where it is compared to the fingerprint forwarded from document verifier terminal 12

or document creation terminal 13 and a "match" or "no match" indication is returned to verification server 10 and on to terminal 12 or 13. In instances where a terminal 12 has no fingerprint reader 14, but a fingerprint is retrieved from a presented document, the fingerprint may be verified in the manner described at the beginning of this paragraph.

In the Detailed Specification, on page 17, the paragraph starting at line 1, replace the paragraph with the following:

Other than information and biometric verification as described in the previous paragraphs, databases associate with trust authorities may still have to be accessed to determine a number of things including if a document applicant or a document presenter is wanted for a crime, and / or is on a watch list including a denied entry list, and / or to determine if there are known concerns about the document applicant, document or document presenter. In such cases, information submitted by the document applicant, or retrieved from the document being verified by document verifier terminal 12 is forwarded via verification system server [[~~10~~]] 11 to an appropriate trust authority server for processing and an indication is returned via server 10 to terminal 12 or 13 indicating if the document applicant or document presenter is wanted for a crime, and / or is on a watch list including a denied entry list, and / or indicating any other known concerns about the document applicant, the document or its presenter.

In the Detailed Specification, on page 17, the paragraph starting at line 14, replace the paragraph with the following:

As may be seen in Fig. 1 there is a homeland security trust authority server [[~~22~~]] 28f that functions to verify information submitted by applicants for a new document, retrieved from issued documents, or

obtained directly from a document presenter with information stored in databases on a secure government network 29, whether that network is a state or federal network. The servers 30-39 for different government agencies are each connected via a gateway 38a-i to the secure government network 29 and are presently used for inter-agency access to data stored in databases on the servers connected to network 29. Trust authority server 22 provides secure, privacy controlled access to information in the databases on servers 30-39 to verify issued documents or their presenters, to verify the identity of document applicants, and to determine if there are any other known concerns about a document applicant, issued document or its presenter. In this way of privacy concerns are adequately met.

In the Detailed Specification, on page 18, the paragraph starting at line 27, replace the paragraph with the following:

In Fig. 2 is a more detailed block diagram of a verification system utilizing trust authorities to access federal, state, private and foreign databases via trust authority servers in a secure manner to verify document applicants, issued documents and individuals to whom the documents are issued, while addressing privacy concerns. In ~~the middle of~~ Fig. [[~~2~~]] 1 is verification system server 10 and verification system communication bus 11 described in the previous paragraphs with reference to Fig. 1. As previously described, server 10 determines which trust authority servers are to be accessed in a secure manner as part of the operation of a document verifier terminal 12 or a document creation terminal 13 in verifying source information from document applicants, issued documents and document presenters. In addition, in some cases, an individual database, such as on transportation reservation / check-in system [~~server~~] servers 25, may not have its own trust authority server and verification system server 10 may act as its trust authority, if a trust authority is

required. All databases requiring a trust authority are accessed via their respective trust authority server 23 - 28, and they are all connected to server 10. All communication paths between these servers are preferably secure communication channels, not accessible from the outside, and over which all communications are encrypted. As previously mentioned information passes between server 10 and all trust authority servers 28, and decisions made at either server 10 or ones of servers 28, is done in a manner to protect privacy of a document applicant at a document creation terminal 13 or document presenter at a document verifier terminal 12.